Recent high profile cyberattacks and data breaches like those suffered by Sony Pictures Entertainment and Target Corporation have prompted many companies to begin reevaluating their own vulnerabilities.

Target's 2013 data breach alone resulted in more than 80 lawsuits and investigations by state and federal agencies, including State Attorneys General, the Federal Trade Commission and the Securities and Exchange Commission. Given the heightened enforcement environment, companies assessing their data-breach response readiness should also have a basic understanding of the various tools that governmental entities can use to investigate data breaches, including the ability to access electronic company data stored by third parties. Generally speaking, state and federal authorities have broad rights to obtain corporate data in connection with criminal and regulatory matters. Those rights are subject to the Electronic Communications Privacy Act and the Fourth Amendment, which the Supreme Court revisited recently in 2014's *Riley v. California*. Nevertheless,

state and federal authorities can pursue virtually any type of data with facially valid legal process, for which process varies depending on the type of data being sought. For example:

- **Subpoenas.** State and federal governmental entities can obtain data via subpoena, although access to electronic communications via subpoena is limited by the Stored Communications Act, which prohibits governmental entities from obtaining content less than 180 days old. Moreover, relevant case law generally requires governmental entities to obtain a search warrant to obtain content, regardless of age. In practice, government entities use subpoenas to obtain basic subscriber information, such as name, address, telephone connection records, and means/source of payment.
- **Search Warrants.** Search warrants can be used to obtain a broad range of data from an investigative target or third party, and may permit the government to seize property (including computers and related equipment) in connection with a criminal investigation.
- **Real-Time Monitoring.** "Pen register" and "trap and trace" device orders permit real-time monitoring of outgoing and incoming dialing or electronic address information, but do not permit access to the *contents* of the communications. However, a wiretap or "Title III" order can be used to intercept the content of wire or electronic communications in real time.
- **User Data**. Under the Stored Communications Act, "2703(d) Orders" permit governmental authorities to obtain "non-content" user data connected with electronic communications, such as clickstream data, log files, user settings, credit information, analytics, email headers, customer service notes, and historic (non-real time) location information if the data is relevant and material to an ongoing criminal investigation. Real time location information requires a wiretap or Title III order, as described above.
- **National Security Letters.** The Director of the Federal Bureau of Investigation can issue National Security Letters to wire providers or electronic communications services to obtain a subscriber's name, address, length of service, and local and long distance toll billing records, in cases where the information sought is relevant to an investigation "to protect against international terrorism or clandestine intelligence activities."

In the case of emergencies, certain process requirements may be lessened or eliminated. For example, an emergency wiretap can be put into place if the Attorney General determines that there is immediate danger of death or serious physical injury, but an order must be applied for within 48 hours. The Government may also ask companies to preserve data in connection with an investigation. Given the broad range of investigative tools readily accessible to these authorities, it is fast becoming an imperative for companies to familiarize themselves with the requirements and limitations of these tools. Companies are increasingly advised to remain cognizant of whether they store sensitive data with third party service providers—such as cloud storage providers—which may be the recipients of investigator demands for company data. As both Wyndham Worldwide Corporation and CBR Systems, Inc. have learned in the wake of their recent cyberattacks, today's data breach victim can often be tomorrow's enforcement target.

Explore more in

White Collar & Investigations
Blog series

White Collar Briefly

Drawing from breaking news, ever changing government priorities, and significant judicial decisions, this blog from Perkins Coie’s White Collar and Investigations group highlights key considerations and offers practical

insights aimed to guide corporate stakeholders and counselors through an evolving regulatory environment.
Subscribe ?

View the blog